APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/961,380	09/25/2001	Ned M. Smith	P 282600 P11801	5485

27496   - 7590   09/27/2005

PILLSBURY WINTHROP SHAW PITTMAN LLP
725 S. FIGUEROA STREET
SUITE 2800
LOS ANGELES, CA 90017

EXAMINER
WILLIAMS, JEFFERY L

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/961,380	SMITH ET AL.
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>08 July 2005</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-21, 23 and 26-31</u> is/are pending in the application.

    4a) Of the above claim(s) <u>22, 24 and 25</u> is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-21, 23 and 26-31</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>11 February 2002</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

1   **DETAILED ACTION**

2

3   This action is in response to the communication filed on 7/8/2005.

4

5   Applicant has amended claims 1 – 21, 23, and 26 – 29. Claims 22, 24, and 25

6   have been cancelled by applicant. Applicant has added claims 30 and 31.

7

8   All objections and rejections not set forth below have been withdrawn.

9

10

11   ***Specification***

12

13   The specification is objected to as failing to provide proper antecedent basis for

14   the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction

15   of the following is required: Claims 2, 5, 7, 12, 19, 27, and 29 do not have proper

16   antecedent basis in the specification. See the rejections of these claims under 35 USC

17   § 112, first paragraph.

18

19

20

21

22

1   *Claim Rejections - 35 USC § 112*

2

3   The following is a quotation of the first paragraph of 35 U.S.C. 112:

4   The specification shall contain a written description of the invention, and of the manner and process of
5   making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the
6   art to which it pertains, or with which it is most nearly connected, to make and use the same and shall
7   set forth the best mode contemplated by the inventor of carrying out his invention.
8
9

10   **Claims 1 – 21, 23, and 26 – 31 are rejected under 35 U.S.C. 112, first**

11   **paragraph, as failing to comply with the written description requirement. The**

12   **claim(s) contains subject matter which was not described in the specification in**

13   **such a way as to reasonably convey to one skilled in the relevant art that the**

14   **inventor(s), at the time the application was filed, had possession of the claimed**

15   **invention.**

16

17   Regarding claim 1, the limitation "wherein the repeating nonce is an action

18   requested in the nonce" is not supported by the specification. The specification does

19   not support the broadly claimed limitation of the repeating nonce being an action

20   requested in the nonce. An action can be a countless number of things. For example,

21   throwing a touchdown pass, robbing a bank, and self-destructing are all actions. The

22   specification as originally presented discloses that the repeating nonce "is consistent

23   with the received nonce", however, it does not disclose the broad limitation that *the*

24   *nonce is a requested action.*

25

1   Regarding claim 6, the limitation "the responding nonce being a response to an

2   action requested by the nonce" is not supported by the specification. An action can be

3   a countless number of things. For example, throwing a touchdown pass, robbing a

4   bank, and self-destructing are all actions. The specification does not support the broadly

5   claimed limitation of the repeating nonce being a *response to an action* requested. The

6   specification as originally presented discloses that the repeating nonce "is consistent

7   with the received nonce", however, it does not disclose the broad limitation *of an action*

8   *requested by a nonce and that the repeating nonce is a response to this action.*

9

10   Regarding claims 10, 14, 21, and 28 the limitation "the repeating nonce including

11   an action requested in the nonce" is not supported by the specification. The

12   specification does not support the broadly claimed limitation of the repeating nonce

13   *including an action requested.* An action can be a countless number of things. For

14   example, throwing a touchdown pass, robbing a bank, and self-destructing are all

15   actions. The specification as originally presented discloses that the repeating nonce "is

16   consistent with the received nonce", however, it does not disclose the broad limitation *of*

17   *an action requested in a nonce and that the repeating nonce includes this action.*

18

19   Regarding claim 18, the limitation "the repeating nonce including a value of an

20   action requested in the nonce" is not supported by the specification. The specification

21   does not support the broadly claimed limitation of the repeating nonce *including a value*

22   *of an action requested.* An action can be a countless number of things. For example,

1   throwing a touchdown pass, robbing a bank, and self-destructing are all actions. The

2   specification as originally presented discloses that the repeating nonce "is consistent

3   with the received nonce", however, it does not disclose the broad limitation *of an action*

4   *requested in a nonce and that the repeating nonce includes a value of this action.*

5   Regarding claim 26 the limitation "a repeating nonce received from the receiver

6   includes an action requested in the nonce sent by the sender" is not supported by the

7   specification. The specification does not support the broadly claimed limitation that the

8   repeating nonce *includes an action requested.* An action can be a countless number of

9   things. For example, throwing a touchdown pass, robbing a bank, and self-destructing

10   are all actions. The specification as originally presented discloses that the repeating

11   nonce "is consistent with the received nonce", however, it does not disclose the broad

12   limitation *of an action requested in a nonce and that the repeating nonce includes this*

13   *action.*

14

15   Regarding claims 2 and 5, the limitation "wherein the repeating nonce is a hand

16   gesture" is not supported by the specification. While the specification discloses a

17   "human gesture" (Applicant's specification, page 10, par. 34), this does not lead one to

18   assume a hand gesture. There are many ways in which a human may "gesture",

19   express an idea, sentiment, attitude, or intention. For example, a human may gesture a

20   state of shame by hanging his/her head (movement of the body), or a human may

21   provide a gesture of sympathy towards a lonely individual with an invitation.

22   Additionally, the disclosure of a "*human* gesture" by the applicant, would not lead one to

1   more broadly conclude a *hand* gesture. A hand may be the forelimb of an animal (such

2   as on an ape or kangaroo), or a mechanical apparatus (such as the indicators on a

3   clock dial), both examples of which are not more narrowly limited to a human hand.

4   Thus, the claimed limitation of a hand gesture, does not find support in the specification.

5

6   Regarding claim 7, the limitation "wherein the repeating nonce is one of a sum of

7   two numbers transmitted as the nonce, multiplication of the two numbers, or a division

8   of the two numbers" does not find support in the applicant's specification. Similarly,

9   claims 12, 19, 27, and 29, contain the limitations "wherein the repeating nonce includes

10   a value corresponding to the addition of two numbers, the two numbers being included

11   in the nonce", "wherein the repeating nonce is a value of an addition of two numbers,

12   the two numbers being originally sent in the nonce", "wherein the repeating nonce is a

13   value of an addition of two numbers, the two numbers being sent in the nonce", and

14   "wherein the repeating nonce is a value of an addition of two numbers, the two numbers

15   being included in the nonce". The examiner does not find support for these limitations

16   within the applicant's specification. The examiner point's out that the applicant has only

17   disclosed in context that an original nonce may be a phrase, "please return the result of

18   37345409394+265350". Further, the applicant has not disclosed that the repeating

19   nonce is the sum of two numbers. At the most, the applicant provides an example

20   disclosing that if the "repeating nonce is not **37345874744**" – *which is not the sum of*

21   *two numbers in the original nonce* - the repeating nonce would not be consistent with

1   the original nonce. Thus, the above mentioned limitations found in claims 7, 12, 19, 27,

2   and 29 are not supported by the applicant's specification.

3

4   All other claims are rejected by virtue of their dependency.

5

6

7

8

9   The following is a quotation of the second paragraph of 35 U.S.C. 112:

10   The specification shall conclude with one or more claims particularly pointing out and distinctly
11   claiming the subject matter which the applicant regards as his invention.
12

13   **Claims 6 – 9 are rejected under 35 U.S.C. 112, second paragraph, as being**

14   **indefinite for failing to particularly point out and distinctly claim the subject**

15   **matter which applicant regards as the invention.**

16

17   The amended claim 6 recites the limitation "the responding nonce" in line 7.

18   There is insufficient antecedent basis for this limitation in the claim. For the purpose of

19   examination, the examiner presumes this limitation to refer to "the repeating nonce".

20

21   Claims 7 – 9 are rejected by virtue of their dependency.

22

23

24

1   *Claim Rejections - 35 USC § 102*

2

3   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

4   form the basis for the rejections under this section made in this Office action:

5   A person shall be entitled to a patent unless –

6   (b) the invention was patented or described in a printed publication in this or a foreign country or in public
7   use or on sale in this country, more than one year prior to the date of application for patent in the United
8   States.
9
10   **Claims 1, 4, 6, 9, 10, 14, 15, 18, and 20 are rejected under 35 U.S.C. 102(b)**

11   **as being anticipated by Schneier, Applied Cryptography.**

12

13   Regarding claim 1, Schneier discloses a method comprising:

14   *sending, from a sender to a receiver, data through a data channel,* the data

15   including a key and a nonce (Schneier, pg. 576, protocol steps 2,3). Data is sent from a

16   sender to a receiver, thus a data channel exists.

17   *receiving, at the receiver, the data* (Schneier, pg. 576, protocol steps 3,4).

18   *establishing a visual physical channel between the sender and the receiver, the*

19   *sender and receiver being visible to each other,* (Schneier, pg. 2, par. 1; pgs. 22,23;

20   pgs. 576, 577). As disclosed by Schneier, the disclosed method deals with computer

21   cryptography. The method is implemented on a computer network with hardware such

22   as PCs or VAXs, and is a communication protocol between senders and receivers on

23   the computer network. Alice and Bob represent the network senders and receivers.

24   Thus, Schneier discloses a physical channel between a sender and receiver.

25   Furthermore, the channel is "visual" (defined as "of, relating to, or used in vision" -

1   Webster's Third New International Dictionary, Unabridged) since the channel allows the

2   sender and receiver on the network to interact and communicate via protocols

3   analogous to human "face-to-face" interaction (Schneier, page 2, par. 5). Thus, the

4   sender and receiver on the network are enabled by the physical channel to interact in a

5   way such that they are "visible" (defined as "recognizable" - Webster's Third New

6   International Dictionary, Unabridged) to each other.

7   *and verifying, between the receiver and the sender via the visual physical*

8   *channel, that the data is from the sender by having the receiver respond by sending a*

9   *repeating nonce to the sender, wherein the repeating nonce is an action requested in*

10   *the nonce* (Schneier, pg. 576, protocol steps 3-5). Schneier discloses an authentication

11   protocol requiring the use of nonces. The use of this protocol includes the sending of a

12   nonce by a sender to a receiver, and the requirement that the receiver return the nonce

13   as a repeating nonce. Thus, the nonce of Schneier, sent from a sender to a receiver,

14   inherently has associated with it the request for the nonce to be repeated ("action") as a

15   repeating nonce.

16

17   Regarding claim 4, Schneier discloses:

18   *wherein after the sender verifies the repeating nonce, the sender sends a signed*

19   *message* (Schneier, page 577, step 17).

20

21   Regarding claims 6 and 10 they contain limitations similar to claim 1, and are

22   rejected for the same reasons.

1

2   Regarding claim 9, Schneier discloses:

3   *sending, from the sender to the receiver, if the verifying is successful, a signed*

4   *message* (Schneier, page 577, step 17).

5

6   Regarding claim 14, it is a system claim containing similar limitations to the

7   corresponding the method of claim 1, and is rejected for the same reasons.

8

9   Regarding claim 15, Schneier discloses:

10   *an information generation mechanism for generating the data, the data including*

11   *the key and the nonce; and* (Schneier, pg. 576, protocol steps 1, 2).

12   *a transmitter for transmitting the data to the receiver via the data channel*

13   (Schneier, pg. 576, protocol step 3).

14

15   Regarding claim 18, it recites the same limitations as claim 15, and is rejected for

16   the same reasons.

17

18   Regarding claim 20, Schneier discloses:

19   *a signed message generation mechanism for generating a signed message to be*

20   *sent, after the verifying, to the receiver through the transmitter, the singed message*

21   *including a signature of the sender* (Schneier, page 577, step 17).

22

1   *Claim Rejections - 35 USC § 103*

2

3   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

4   obviousness rejections set forth in this Office action:

5   (a) A patent may not be obtained though the invention is not identically disclosed or described as set
6   forth in section 102 of this title, if the differences between the subject matter sought to be patented and
7   the prior art are such that the subject matter as a whole would have been obvious at the time the
8   invention was made to a person having ordinary skill in the art to which said subject matter pertains.
9   Patentability shall not be negatived by the manner in which the invention was made.
10
11   **Claims 5, 13, 16, 17, 21, 23, 26, and 28 are rejected under 35 U.S.C. 103(a) as**

12   **being unpatentable over Schneier, <u>Applied Cryptography</u>.**

13

14   Regarding claims 5 and 13, Schneier discloses:

15   *receiving, at the receiver,* (a/the) *signed message, and verifying* (a/the) *signature*

16   *in the signed message using the stored key* (Schneier, page 577, steps 17 and 18).

17   Schneier does not disclose *storing, by the receiver, the key received from the sender as*

18   *a stored key, if the verifying is successful.*

19   However, it is logical that a receiver, desiring a verified key for communication,

20   would proceed to store (instead of discarding) the key in memory for future use if it were

21   verified. Notice, the key obtained by the receiver in step 4 is employed at a later time by

22   the receiver in step 18. Hence, Schneier implies using the stored key. Therefore, it

23   would have been obvious to one of ordinary skill in the art, based upon logical

24   reasoning, to recognize that Schneier implies storing the key if it were verified, because

25   a receiver desiring to employ a verified key would store the verified key for future use.

26

1   Regarding claim 16, the Schneier discloses:

2   a transmission receiver for intercepting the data, sent from the sender through

3   the data channel *(Schneier, pg. 576, protocol steps 3,4). As explained in claim 1, Alice*

4   *and Bob represent senders and receivers on a computer network. Thus, Schneier,*

5   *discloses a transmission receiver (Bob).*

6   Schneier does not disclose *a key storage for storing a key included in the*

7   *received data, if the verifying is successful.*

8   However, as explained regarding claim 13, it is logical that a receiver, desiring a

9   verified key for communication, would proceed to store (instead of discarding) the key in

10   memory for future use if it were verified. Notice, the key obtained by the receiver in step

11   4 is employed at a later time by the receiver in step 18. Hence, Schneier implies using

12   the stored key. Therefore, it would have been obvious to one of ordinary skill in the art,

13   based upon logical reasoning, to recognize that Schneier implies storing the key if it

14   were verified, because a receiver desiring to employ a verified key would store the

15   verified key for future use.

16

17   Regarding claim 17, the qualification of Schneier discloses:

18   *the sender further including a signed message generation mechanism for*

19   *generating a signed message to be sent, after the verifying, to the receiver through the*

20   *transmitter, the signed message including a signature of the sender and the receiver*

21   *further comprising a signature verification mechanism for verifying, upon receiving the*

22   *signed message, the signature of the sender received through the transmission receiver*

1   (Schneier, pgs. 576, 577, protocol steps 1, 2, 3, 17). Schneier discloses that the sender

2   comprises the ability to generate data and construct a message, the message bearing

3   the signature of the sender.

4

5   Regarding claims 21 and 23, they contain similar limitations as claim 17, and

6   they are rejected for the same reasons.

7

8   Regarding claim 26, the qualification of Schneier, as explained regarding claims

9   13, 16, 17, 21, and 23, does not disclose a computer-readable medium encoded with a

10   program. However, it is obvious that the sending and receiving computers of data on

11   the computer network disclosed by Schneier would comprise a medium encoded with

12   computer instructions. Thus, it would have been obvious to one of ordinary skill in the

13   art to recognize that the qualification of Schneier would contain computer readable

14   medium encoded with a program because a network of operating computers could not

15   operate without computer instructions embodied in a medium.

16   Therefore, the qualification of Schneier discloses:

17   *send, from a sender to a receiver, data through a data channel, the data*

18   *including a key and a nonce* (Schneier, pg. 576, protocol step 3).

19   *send, from the sender to the receiver a signed message, after verifying, via a*

20   *physical channel, that the data received by the receiver is from the sender by verifying*

21   *that a repeating nonce received from the receiver includes an action requested in the*

1   *nonce sent by the sender* (Schneier, pg. 577, protocol steps 16, 17, see rejection of

2   claim 1).

3

4   Regarding claim 28, it contains limitations similar to claims 21, 23, and 26, and is

5   rejected for the same reasons.

6

7   **Claims 30 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable**

8   **over the qualification of Schneier as applied to claims 5, 13, 16, 17, 21, 23, 26, and**

9   **28 above, and further in view of Callas, "Using and Creating Cryptographic-**

10   **Quality Random Numbers".**

11

12   Regarding claims 30 and 31, Schneier discloses the use of nonces in an

13   authentication protocol. These nonces are random numbers generated by a sender.

14   The nonce, or random number, is sent from a sender to a receiver. The sole purpose of

15   the nonce is for purposes of verification by retransmitting the received nonce as a

16   repeated nonce. Thus, a received nonce is appropriately viewed as a request to

17   transmit a consistent repeated nonce (Schneier, pages 576-577). Schneier, however,

18   does not disclose how a sender generates a random number for a nonce. Schneier

19   does not disclose *wherein the repeating nonce is an audio signal,* or *an audio signal*

20   *including a phrase spoken in a language requested in the nonce.*

21   Callas discloses that random numbers may be generated in a variety of ways.

22   On computers, random numbers are unpredictable streams or strings of bits (Callas,

1   page 1). Callas discloses that audio signals may be used as random numbers. Audio

2   signals may be gathered by a microphone from a variety of input sources, such as

3   sound sources in a room. (Callas, pages 2 and 3). Callas further discloses that the best

4   source of entropic inputs is people or users. It is advantageous for random numbers to

5   be collected from the inputs of a user, as users are the most entropic, or most random,

6   sources available (Callas, page 3, par. 2).

7   It would have been obvious to one of ordinary skill in the art to combine the

8   teachings of Callas for using audio signals and user inputs as random numbers. This

9   would have been obvious because one of ordinary skill in the art would have been

10   motivated to provide a way to efficiently generate "quality" random numbers.

11   Thus the combination of Schneier and Callas discloses a nonce, and by

12   extension, a repeating nonce, consistent with the nonce as being an audio signal

13   translated into a unpredictable string of bits. Furthermore, it is well known that people

14   can create audible signals within a room using phrases spoken in a language. Callas

15   discloses that any audible signals within a room can be collected as a random number.

16   Thus, the combination of Schneier and Callas also disclose a nonce, and by extension a

17   requested repeating nonce, as being an audio signal including a phrase spoken in a

18   language.

19

20

21

22

1   **Claims 2, 3, 8, and 11 are rejected under 35 U.S.C. 103(a) as being**

2   **unpatentable over Schneier as applied to claims 1, 4, 6, 9, 10, 14, 15, 18, and 20**

3   **above, and further in view of Callas, "Using and Creating Cryptographic-Quality**

4   **Random Numbers".**

5

6   Regarding claim 2, Schneier discloses the use of nonces in an authentication

7   protocol. These nonces are random numbers generated by a sender. The nonce, or

8   random number, is sent from a sender to a receiver. The sole purpose of the nonce is

9   for purposes of verification by retransmitting the received nonce as a repeated nonce.

10   Thus, a received nonce is appropriately viewed as a request to transmit a consistent

11   repeated nonce (Schneier, pages 576-577). Schneier, however, does not disclose how

12   a sender generates a random number for a nonce. Schneier does not disclose *wherein*

13   *the repeating nonce is a hand gesture..*

14   Callas discloses that random numbers may be generated in a variety of ways.

15   On computers, random numbers are unpredictable streams or strings of bits (Callas,

16   page 1). Callas discloses that the best source of entropic inputs is people or users.

17   Callas discloses that as a user types, his keystrokes may be used as random numbers.

18   (Callas, pages 2 and 3). It is advantageous for random numbers to be collected from

19   user inputs, as users are the most entropic, or most random, sources available (Callas,

20   page 3, par. 2).

21   It would have been obvious to one of ordinary skill in the art to combine the

22   teachings of Callas for using hand gestures or keystrokes as random numbers. This

1   would have been obvious because one of ordinary skill in the art would have been

2   motivated to provide a way to efficiently generate "quality" random numbers.

3

4   Regarding claims 3, 8, and 11 Schneier discloses the use of nonces in an

5   authentication protocol. These nonces are random numbers generated by a sender.

6   The nonce, or random number, is sent from a sender to a receiver. The sole purpose of

7   the nonce is for purposes of verification by retransmitting the received nonce as a

8   repeated nonce. Thus, a received nonce is appropriately viewed as a request to

9   transmit a consistent repeated nonce (Schneier, pages 576-577). Schneier, however,

10   does not disclose how a sender generates a random number for a nonce. Schneier

11   does not disclose *wherein the repeating nonce is an audio signal,* or *an audio signal*

12   *including a phrase spoken in a language requested in the nonce.*

13   Callas discloses that random numbers may be generated in a variety of ways.

14   On computers, random numbers are unpredictable streams or strings of bits (Callas,

15   page 1). Callas discloses that audio signals may be used as random numbers. Audio

16   signals may be gathered by a microphone from a variety of input sources, such as

17   sound sources in a room. (Callas, pages 2 and 3). Callas further discloses that the best

18   source of entropic inputs is people or users. It is advantageous for random numbers to

19   be collected from user inputs, as users are the most entropic, or most random, sources

20   available (Callas, page 3, par. 2).

21   It would have been obvious to one of ordinary skill in the art to combine the

22   teachings of Callas for using audio signals and user inputs as random numbers. This

1   would have been obvious because one of ordinary skill in the art would have been

2   motivated to provide a way to efficiently generate "quality" random numbers.

3   Thus the combination of Schneier and Callas discloses a nonce, and by

4   extension, a repeating nonce, consistent with the nonce as being an audio signal

5   translated into a unpredictable string of bits. Furthermore, it is well known that people

6   can create audible signals within a room using phrases spoken in a language. Callas

7   discloses that any audible signals within a room can be collected as a random number.

8   Thus, the combination of Schneier and Callas also disclose a nonce, and by extension a

9   requested repeating nonce, as being an audio signal including a phrase spoken in a

10   language.

11

12

13   **Claims 7, 12, and 19 are rejected under 35 U.S.C. 103(a) as being**

14   **unpatentable over Schneier as applied to claims 1, 4, 6, 9, 10, 14, 15, 18, and 20**

15   **above, and further in view of Menezes et al., "Handbook of Applied**

16   **Cryptography".**

17

18   Regarding claim 7, Schneier discloses the use of nonces in an authentication

19   protocol (Schneier, pages 576-577). Schneier does not disclose *wherein the repeating*

20   *nonce is one of a sum of two numbers transmitted as the nonce; a multiplication of the*

21   *two numbers, or a division of the two numbers.*

1   Menezes et al., however, discloses that discloses that there are disadvantages

2   when using random numbers as nonces in authentication protocols (Menezes et al.,

3   remark 10.12). Thus, Menezes et al. shows that sequence numbers may be used as

4   nonces instead (Menezes et al., (ii)). Therefore, Menezes et al. discloses a nonce

5   being the *sum of two numbers* (a sequence number + a prior sequence number)

6   transmitted in the nonce.

7   It would have been obvious to one of ordinary skill in the art to combine the

8   teaching of Menezes et al. with the method of Schneier. This would have been obvious

9   because one of ordinary skill in the art would have been motivated to use sequence

10   numbers as nonces so as to avoid the disadvantages of using random numbers.

11

12   Claims 12 and 19 contain limitations similar to claim 7, and they are rejected for

13   the same reasons.

14

15   **Claims 27 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable**

16   **over the qualification of Schneier as applied to claims 5, 13, 16, 17, 21, 23, 26, and**

17   **28 above, and further in view of Menezes et al., "Handbook of Applied**

18   **Cryptography".**

19

20   Regarding claim 27, Schneier discloses the use of nonces in an authentication

21   protocol (Schneier, pages 576-577). Schneier does not disclose *wherein the repeating*

1   *nonce is a value of an addition of two numbers, the two numbers being sent in the*

2   *nonce.*

3   Menezes et al., however, discloses that discloses that there are disadvantages

4   when using random numbers as nonces in authentication protocols (Menezes et al.,

5   remark 10.12). Thus, Menezes et al. shows that sequence numbers may be used as

6   nonces instead (Menezes et al., (ii)). Therefore, Menezes et al. discloses a nonce

7   being the *sum of two numbers* (a sequence number + a prior sequence number)

8   transmitted in the nonce.

9   It would have been obvious to one of ordinary skill in the art to combine the

10   teaching of Menezes et al. with the method of Schneier. This would have been obvious

11   because one of ordinary skill in the art would have been motivated to use sequence

12   numbers as nonces so as to avoid the disadvantages of using random numbers.

13

14   Claims 29 contain limitations similar to claim 27, and it is rejected for the same

15   reasons.

16

17

18

19

20

21

22

1   *Response to Arguments*

2

3   Applicant's arguments with respect to claims 1 – 21, 23, and 26 – 29 have been

4   considered but are moot in view of the new ground(s) of rejection.

5

6   *Conclusion*

7

8   The prior art made of record and not relied upon is considered pertinent to

9   applicant's disclosure:

10   Webster's Third New International Dictionary, Unabridged, Definitions for "hand",

11   "visible", "vision", "visual", "gesture",1993, Merriam-Webster.

12   Ritter,Terry; "Random Noise Sources", 1999,

13   http://www.ciphersbyritter.com/NOISE/NOISRC.HTM, accessed 9/20/05.

14   Ellison, Carl, "Cryptographic Random Numbers", April 2001,

15   http://world.std.com/~cme/P1363/ranno.html, accessed 9/20/05.

16   Bruce Schneier, Applied Cryptography, 1996, John Wiley & Sons, Inc., 2nd ed.,

17   page 575.

18

19   Applicant's amendment necessitated the new ground(s) of rejection presented in

20   this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

21   § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

22   CFR 1.136(a).

1   A shortened statutory period for reply to this final action is set to expire THREE

2   MONTHS from the mailing date of this action. In the event a first reply is filed within

3   TWO MONTHS of the mailing date of this final action and the advisory action is not

4   mailed until after the end of the THREE-MONTH shortened statutory period, then the

5   shortened statutory period will expire on the date the advisory action is mailed, and any

6   extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

7   the advisory action. In no event, however, will the statutory period for reply expire later

8   than SIX MONTHS from the date of this final action.

9

10   Any inquiry concerning this communication or earlier communications from the

11   examiner should be directed to Jeffery Williams whose telephone number is (571) 272-

12   7965. The examiner can normally be reached on 8:30-5:00.

13   If attempts to reach the examiner by telephone are unsuccessful, the examiner's

14   supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

15   number for the organization where this application or proceeding is assigned is 571-

16   273-8300.

1   Information regarding the status of an application may be obtained from the

2   Patent Application Information Retrieval (PAIR) system. Status information for

3   published applications may be obtained from either Private PAIR or Public PAIR.

4   Status information for unpublished applications is available through Private PAIR only.

5   For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

6   you have questions on access to the Private PAIR system, contact the Electronic

7   Business Center (EBC) at 866-217-9197 (toll-free).

8

9
10 Jeffery Williams
11 Assistant Examiner
12 AU: 2137
13
14   EMMANUEL L. MOISE
15   SUPERVISORY PATENT EXAMINER